

A

PTO/SB/05 (08-00)  
Approved for use through 10/31/2002. OMB 0651-0033  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UTILITY  
PATENT APPLICATION  
TRANSMITTAL

*(Only for new nonprovisional applications under 37 CFR 1.53(b))*

Attorney Docket No. CISCO-3095

|                |              |
|----------------|--------------|
| First Inventor | Sheth et al. |
|----------------|--------------|

|       |                                 |
|-------|---------------------------------|
| Title | PPP Doamin Name and L2TP Tunnel |
|-------|---------------------------------|

Express Mail Label No. **EL575422536US**

## APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents  
Box Patent Application  
Washington, DC 20231

1. ☐ Fee Transmittal Form (e.g., PTO/SB/77)  
(Submit an original and a duplicate for fee processing)
2. ☐ Applicant claims small entity status.  
See 37 CFR 1.27.
3. ☒ Specification [Total Pages (preferred arrangement set forth below)
- Descriptive title of the invention
  - Cross Reference to Related Applications
  - Statement Regarding Fed sponsored R & D
  - Reference to sequence listing, a table,  
or a computer program listing appendix
  - Background of the Invention
  - Brief Summary of the Invention
  - Brief Description of the Drawings (if filed)
  - Detailed Description
  - Claim(s)
  - Abstract of the Disclosure
4. ☒ Drawing(s) (35 U.S.C. 113) [ Total Sheets 

5. Oath or Declaration [ Total Pages  ]

a. ☐ Newly executed (original or copy)

b. ☐ Copy from a prior application (37 CFR 1.63 (d))  
(for continuation/divisional with Box 17 completed)

i. ☐ DELETION OF INVENTOR(S)  
Signed statement attached deleting inventor(s)  
named in the prior application, see 37 CFR  
1.63(d)(2) and 1.33(b).

6. ☐ Application Data Sheet. See 37 CFR 1.76

7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (*Appendix*)
8. Nucleotide and/or Amino Acid Sequence Submission (*if applicable, all necessary*)
- a. ☐ Computer Readable Form (CRF)
- b. Specification Sequence Listing on:
- i. ☐ CD-ROM or CD-R (2 copies); or
- ii. ☐ paper
- c. ☐ Statements verifying identity of above copies

## ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers (cover sheet & document(s))
10. ☐ 37 CFR 3.73(b) Statement ☐ Power of Attorney  
(when there is an assignee)
11. ☐ English Translation Document (if applicable)
12. ☐ Information Disclosure ☐ Copies of IDS  
Statement (IDS)/PTO-1449 Citations
13. ☐ Preliminary Amendment
14. ☒ Return Receipt Postcard (MPEP 503)  
(Should be specifically itemized)
15. ☐ Certified Copy of Priority Document(s)  
(if foreign priority is claimed)
16. ☐ Other: \_\_\_\_\_

17. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP)

of prior application No.: \_\_\_\_\_ / \_\_\_\_\_

**Prior application information:**

Examiner \_\_\_\_\_

Group / Art Unit: \_\_\_\_\_

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

## 18. CORRESPONDENCE ADDRESS

Customer Number or Bar Code Label

or ☐ Correspondence address below

|      |                  |
|------|------------------|
| Name | David B. Ritchie |
|------|------------------|

D'Alessandro &amp; Ritchie

|         |                  |
|---------|------------------|
| Address | P. O. Box 640640 |
|---------|------------------|

|      |          |       |    |          |       |
|------|----------|-------|----|----------|-------|
| City | San Jose | State | CA | Zip Code | 95164 |
|------|----------|-------|----|----------|-------|

|                |     |                  |              |            |              |
|----------------|-----|------------------|--------------|------------|--------------|
| <i>Country</i> | USA | <i>Telephone</i> | 408-441-1100 | <i>Fax</i> | 408-441-8400 |
|----------------|-----|------------------|--------------|------------|--------------|

Name (Print/Type) John P. Schaub

|                                   |        |
|-----------------------------------|--------|
| Registration No. (Attorney/Agent) | 42.125 |
|-----------------------------------|--------|

*Signature*

Date **11/13/00**

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Sheth et al.  
SERIAL NO.: (not yet assigned)  
FILING DATE: November 13, 2000  
TITLE: PPP DOMAIN NAME AND L2TP TUNNEL SELECTION  
CONFIGURATION OVERRIDE  
EXAMINER: [not yet assigned]  
ART UNIT: [not yet assigned]



CERTIFICATE OF MAILING

"Express Mail" mailing label no.: EL575422536US

Date of Deposit: November 13, 2000

I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated above and addressed to:  
Box PATENT APPLICATION, Commissioner for Patents, Washington, DC 20231, on the date printed below:

Name: Diane Morse  
Diane Morse

BOX PATENT APPLICATION  
COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

TRANSMITTAL LETTER

Enclosed for filing please find the patent application for an invention entitled, "PPP DOMAIN NAME AND L2TP TUNNEL SELECTION CONFIGURATION OVERRIDE", filed on behalf of Cisco Technology, Inc., assignee from inventors Purnam Sheth, Aravind Sitaraman, Charles Yager, and Gregory Burns, including Utility Patent Application Transmittal, 22 pages of specification, 9 pages of claims, 9 sheets of drawing figures, and 1 page of Abstract.

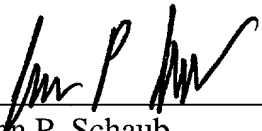
The attorney's Docket Number is CISCO-3095.

Please address all communications regarding this application to:

David B. Ritchie  
D'Alessandro & Ritchie  
P.O. Box 640640  
San Jose, CA 95164-0640  
Telephone (408) 441-1100

No fee is being paid at this time.

Respectfully submitted,  
D'ALESSANDRO & RITCHIE

  
\_\_\_\_\_  
John P. Schaub  
Reg. No. 42,125

Dated: November 13, 2000

D'Alessandro & Ritchie  
P.O. Box 640640  
San Jose, CA 95164-0640  
(408) 441-1100

**UNITED STATES PATENT APPLICATION**

**FOR**

**PPP DOMAIN NAME AND L2TP TUNNEL SELECTION CONFIGURATION  
OVERRIDE**

**INVENTORS:**

**PURNAM SHETH  
ARAVIND SITARAMAN  
CHARLES YAGER  
GREGORY BURNS**

**ASSIGNED TO:**

**CISCO TECHNOLOGY, INC.**

**PREPARED BY:**

**D'ALESSANDRO & RITCHIE  
P.O. BOX 640640  
SAN JOSE, CA 95164-0640  
TELEPHONE: (408) 441-1100  
FAX: (408) 441-8400**

SPECIFICATION

TITLE OF INVENTION

5        PPP DOMAIN NAME AND L2TP TUNNEL SELECTION CONFIGURATION  
             OVERRIDE

BACKGROUND OF THE INVENTION

10    Cross Reference to Related Applications

         This application is related to the following:

         U.S. Patent Application Serial No. 09/488,394, filed January 20, 2000 in the name of  
         inventors Aravind Sitaramin, Aziz Abdul, Bernard Janes, Dennis Cox, John Joyce, Peter  
         Heitman, Shujin Zhang and Rene Tio, entitled "System and Method for Identifying a  
15    Subscriber for Connection to a Communication Network", commonly assigned herewith.

         U.S. Patent Application Serial No. 09/488,395, filed January 20, 2000 in the name of  
         inventors Aravind Sitaramin, Dennis Cox, John Joyce and Shujin Zhang, entitled  
         "System and Method for Determining Subscriber Information", commonly assigned  
         herewith.

20    U.S. Patent Application Serial No. \_\_\_\_\_, filed November 13, 2000 in the name  
         of inventors Purnam Sheth, Aravind Sitaraman, Charles Yager and Gregory Burns,  
         entitled "PPP/L2TP Domain Name Pre-Authorization", commonly assigned herewith.

Field of the Invention

The present invention relates to the field of data communications. More particularly, the present invention relates to a system and method for static selection of  
5 tunnel-based network connections.

The Background Art

A significant concern of the individual private and public domains making up the Internet or any other system incorporating multiple networks is the ability to ensure that  
10 only those subscribers who are authorized to access the individual private and public domains within the comprehensive network have the capability to access such networks. Serious security risks are posed by the possibility of unauthorized users having the know-how and capability to invade the individual private and public domains within the network.

15

In today's networking environment, many privately owned domain sites exist on the Internet that allow access only to those individuals which have been granted the proper authorization. For example, these may include company owned private domains containing confidential information and, as such, the company may grant access only to  
20 those employed by the company, or they may be communities of interest (i.e. "pay-sites") that provide information only to those subscribers which subscribe to the privately owned domain. The subscriber who connects to the Internet, typically by means of an Internet Service Provider (ISP) or Telephone Company (Telco), may also possess the capability to

assume the identity of an authorized user. This capability heightens the potential for security violations.

5           Additionally, it is becoming increasingly more prevalent for individual computer users to have the capability to remotely access privately owned intra networks. Such Virtual Private Networks (VPNs) allow the user to connect with the private intra network of the company from the user's residence by means of the telephone line or other convenient means. The inception of wireless remote connections have even made it possible for users to connect from almost any imaginable locale. The ability to connect remotely to individual private intra networks, once seen as a luxury, has become so commonplace that many working professionals require such access in order to accomplish their everyday job assignments. In many instances, remote users connect to privately owned intra networks through the same means that individuals connect to the Internet, typically Telcos or ISPs. VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This reduces overhead costs associated with traditional remote access methods.

Figure 1 shows a simplified diagram of a computer user connected to a computer network 10 via a host computer 12 linked to an access point 14 which grants authorization to external networks or domains 16, 18 and 20. The potential for a network security violation is posed by the user having the capability through the access point 14 to reach or “Knock on the door” of home gateways 22, 24 and 26.

Still referring to Fig. 1, the user has access to the computer networks through a workstation or host computer 12. The host computer 12 has the capability to connect with the external networks through an access point 14. An access point 14 is essentially an external location capable of permitting authorized users to access external computer networks. Typically, the access point consists of a series of Network Access Servers (NASs) and other related hardware, software and/or firmware. An access point 14 may also include a modem pool (not shown) maintained by a Telephone Company (Telco) or an Internet Service Provider (ISP) which enables its authorized users or subscribers to obtain external network access through the host computer 12 which has the required dial-up connection capability. Those of ordinary skill in the art will recognize that other types of access methods may be provided by a Telcos or ISP such as frame relay, leased lines, ATM (Asynchronous Transfer Mode), ADSL (Asymmetric Digital Subscriber Line) and the like.

Typically, when the user desires to access a specified domain, such as the first privately owned secured domain site 16, the user runs a network logon application program on the host computer 12 which requires the user to input user identification and authorization information as a means of initiating access to the desired network. This information is then directed to the access point 14 where it is verified to ensure that the host user has the required authorization to permit access to the desired network. Once authorization is granted to the user, a connection is established via the access point 14 with the home gateway 22 of the specified first privately owned secure domain site 16. The connection established may be a tunnel-based connection, such as L2TP (Layer Two



Tunneling Protocol) or L2F (Layer Two Forwarding), or an IP-based (Internet Protocol) connection, such as used with ATM or frame relay. The user of the host computer 12, having established such a connection, has the ongoing capability to access the specified domain until the connection is terminated either at the directive of the user or by error in data transmission. The access point 14 will typically have the capability to connect the user to various other privately owned secured domain sites, such as the second private domain site 18 or the public Internet 20. The user of the host computer 12 may use the PPP protocol to connect through the wholesaler networks to another Home Gateway.

Layer 2 Tunneling Protocol (L2TP) is used in many Virtual Private Networks (VPNs). An L2TP access concentrator (LAC) is a device that the client directly connects to and that tunnels Point-to-Point (PPP) frames to the L2TP network server (LNS). The LAC is the initiator of incoming calls and the receiver of outgoing calls. An L2TP network server (LNS) is the Termination point for an L2TP tunnel and the access point where PPP frames are processed and passed to higher layer protocols. The LNS handles the server side of the L2TP protocol. The LNS terminates calls arriving at any of the LAC's PPP interfaces, including asynchronous, synchronous and ISDN. The LNS is the initiator of outgoing calls and the receiver of incoming calls.

Figure 2 is a block diagram that illustrates an L2TP tunnel and how a user typically connects to a privately owned domain site such as a corporate intranet. Using L2TP tunneling, an L2TP access concentrator (LAC) 100 located at the ISP's point of presence (POP) 105 exchanges PPP messages 110 with remote users 115 and

communicates by way of L2TP requests and responses with the customer's L2TP network server (LNS) 120 to set up tunnels 125. The L2TP protocol passes protocol-level packets through the virtual tunnel 125 between end points of a point-to-point connection. Frames  
 5 from remote users are accepted by the ISP's POP 105, stripped of any linked framing or transparency bytes, encapsulated in L2TP and forwarded over the appropriate tunnel 125. The customer's home gateway 120 accepts these L2TP frames, strips the L2TP encapsulation, and processes the incoming frames for the appropriate interface.

10 Turning now to Fig. 3 a block diagram that illustrates the use of AAA servers in an L2TP tunneling network is presented. The selection of the L2TP tunnel 200 at the LAC 205 or NAS is typically determined by an authentication, authorization and accounting (AAA) server 210 based upon the structured username (username@domain) in the PPP authentication packet. The AAA 210 looks up a service profile that matches  
 15 the domain name string. The service profile includes the IP address of the L2TP network server (LNS) 215 and a password for the tunnel 200. Once tunnels are established, the LAC 205 forwards the subscriber's PPP session to the destination LNS 215 through the L2TP tunnel 200. The ISP or enterprise customer 220 receives new PPP sessions and authenticates the sessions using AAA server 225. Authenticated sessions are established  
 20 on the LNS 215, while sessions that fail authentication are rejected.

Present methods of establishing a tunnel allow an unauthorized user to reach or "Knock on the door" of another Home Gateway 215, merely by changing the domain name provided in the PPP authentication packet to the domain name of the intended

Home Gateway 215. In this scenario, all users having access to access point 205 would have the potential to reach the privately owned secured domain site. For example, a user having a domain name of xxx@corpA.com may change the domain name in the PPP

- 5 authentication packet to xxx@corpB.com, allowing the user's PPP session to be forwarded to the corpB LNS through the L2TP tunnel assigned to corpB. Allowing such unauthorized access to a Home Gateway 215 subjects the Home Gateway 215 to potential security risks, including denial of service attacks.

- 10 Denial-of-service attacks typically focus on making a service unavailable for normal use, which is often accomplished by exhausting a resource limitation on the network or within an operating system or application. When involving specific network server applications, these attacks can focus on acquiring and keeping open all of the available connections supported by that server, effectively locking out valid users of the
- 15 server or service. For example, a user intending to exploit present day L2TP systems could flood the network with many PPP sessions targeted to a Home Gateway for which the user is not authorized. Although the LNS authentication process would typically prevent an unauthorized user from access to the corporate intranet, the resources devoted to handling the large number of PPP sessions could adversely affect the services available
- 20 to authorized users.

The currently available solutions to this problem are very limited and do not offer the level of security protection that most companies operating secured and confidential private intra networks demand. Companies have been able to minimize the risk by

setting up internal access points which effectively cause the user/host to dial-in or  
connect directly with the private intra network without going through an external ISP or  
Telco. While this direct-connect service allows some measure of security it does so at the  
5 expense of increasing the costs associated with maintaining an internal access point and  
the additional connection costs related to remote users having to potentially incur long  
distance telephone service charges.

What is needed is a solution that prevents unauthorized PPP sessions from being  
10 forwarded to a destination LNS. A further need exists for such a solution that does not  
alter the original PPP authentication packet.

15

BRIEF DESCRIPTION OF THE INVENTION

A method for controlling subscriber access in a network capable of establishing  
5 connections with multiple services includes receiving a communication from a subscriber  
using a first communication network coupled to a second communication network, the  
communication optionally including a domain identifier associated with a service on the  
second communication network, and authorizing the subscriber to access a service on the  
second communication network using a virtual circuit. The authorization is based upon a  
10 domain configuration override attribute associated with the virtual circuit used to receive  
the communication from the subscriber. An access server capable of forcing subscribers  
of a communications system to gain access exclusively to a domain network associated  
with a virtual circuit includes an authorizer to grant service authorization to the  
subscribers based upon a virtual circuit used to make a service request, a virtual circuit  
15 profile request generator to generate virtual circuit profile requests and a calculator to  
determine whether the service associated with the virtual circuit matches the service  
associated with a domain configuration override attribute.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a computer network wherein the host computer has  
5 access to multiple domains within the network.

Fig. 2 is a block diagram that illustrates an L2TP tunnel and how a user typically  
connects to a corporate intranet.

10 Fig. 3 is a block diagram that illustrates the use of AAA servers in an L2TP  
tunneling network.

Fig. 4 is a block diagram of a differentiated computer network that has the  
capability to force subscribers of the system to gain access exclusively to a domain  
15 network associated with a virtual circuit in accordance with one embodiment of the  
present invention.

Fig. 5 is a flow diagram that illustrates a method for static configuration of tunnel-  
based network connections in accordance with one embodiment of the present invention.  
20

Fig. 6 is a flow diagram that illustrates a method for static configuration of tunnel-  
based network connections in accordance with one embodiment of the present invention.

Fig. 7 is a flow diagram that illustrates a method for determining the domain name associated with virtual circuit in accordance with one embodiment of the present invention.

5

Fig. 8 is a flow diagram that illustrates a method for determining the tunnel ID associated with a virtual circuit in accordance with one embodiment of the present invention.

10

Fig. 9A is a virtual circuit profile table that illustrates tunnel configuration information that may be stored in accordance with one embodiment of the present invention.

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000

15

Fig. 9B is a table that includes a list of tunnel IDs and associated virtual circuit identifiers in accordance with one embodiment of the present invention.

Fig. 9C is a virtual circuit profile table that illustrates tunnel configuration information that may be stored in accordance with one embodiment of the present invention.

20

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Those of ordinary skill in the art will realize that the following description of the  
5 present invention is illustrative only and not in any way limiting. Other embodiments of  
the invention will readily suggest themselves to such skilled persons having the benefit of  
this disclosure.

In accordance with a presently preferred embodiment of the present invention, the  
10 components, processes and/or data structures may be implemented using C++ programs  
running on high performance computers (such as an Enterprise 2000™ server running  
Sun Solaris™ as its operating system. The Enterprise 2000™ server and Sun Solaris™  
operating system are products available from Sun Microsystems, Inc. of Mountain View,  
California). Different implementations may be used and may include other types of  
15 operating systems, computing platforms, computer programs, firmware and/or general  
purpose machines. In addition, those of ordinary skill in the art will readily recognize  
that devices of a less general purpose nature, such as hardwired devices, devices relying  
on FPGA (field programmable gate array) or ASIC (Application Specific Integrated  
Circuit) technology, or the like, may also be used without departing from the scope and  
20 spirit of the inventive concepts disclosed herein.

The authentication, authorization and accounting (AAA) service performs user  
authentication, user authorization and user accounting functions. It may be a Cisco  
ACST™ product such as Cisco Secure™, available from Cisco Systems, Inc. of San Jose,



California, or an equivalent product. In accordance with one embodiment of the present invention, the Remote Authentication Dial-In User Service (RADIUS) protocol is used as the communication protocol for carrying AAA information. RADIUS is an Internet  
 5 standard track protocol for carrying authentication, authorization, accounting and configuration information between devices that desire to authenticate their links and a shared AAA or AAA proxy service. Those of ordinary skill in the art will realize that other authentication protocols such as TACACS+ or DIAMETER can be used as acceptable authentication communications links between the various communications  
 10 devices that encompass the data communications network and still be within the inventive concepts disclosed herein.

Turning now to Fig. 4, a block diagram that illustrates a communication system 300 in accordance with one embodiment of the present invention is presented. Users  
 15 connect to public or private domain networks within communication system 300 through host computers 305, 310, 315. The host computers 305, 310, 315 have the capability to connect or link with domain 320. Domain 320 may be a private domain or a public domain, such as the Internet or a private intra network. These links or connections are established via a series of hardware that serve to grant access to specific domains and  
 20 transport data packets to and from the host computers 305, 310, 315 and domain 320.

The host computers 305, 310, 315 in this particular computer network are connected to a Publicly Switched Telephone Network (PSTN) 325 via a transmission means 330, 335, 340, such as copper wire or cable. Broadcast mechanisms such as

ADSL (Asymmetric Digital Subscriber Line) may be used. Those of ordinary skill in the art will recognize that other types of broadcast mechanisms may be provided by an ISP or Telco such as Ethernet<sup>TM</sup>, frame relay, leased lines, ATM (Asynchronous Transfer Mode) or the like. Access points 345 are located within a wide area network (WAN) 350 and are operated by Telcos or ISPs. The access points 345 house AAA servers 355, Service Selection Gateways (not shown in Fig. 4), L2TP Access Concentrators (LACs) 360, Digital Subscriber Line Aggregation Multiplexers (DSLAMs) 365, 370, 375 or similar devices. The Service Selection Gateway (SSG) is not an integral part of the present invention and therefore a discussion related to their functionality would not benefit the discussion of the present invention. The SSG serves as a gateway between the user and public area domains, such as the Internet.

In order for a user host to gain access to a public domain network, such as the Internet, users must first dial-in or otherwise make a connection with the SSG through a data-receiving interface (not shown in Fig. 5.). As a threshold matter, an authorizer (not shown in Fig. 5) within the LAC serves to authenticate the identity of the user, ensure authorization and ascertain the nature and scope of the public network services that it will provide.

According to one embodiment of the present invention, an access point 345 includes one or more DSLAMs 365, 370, 375 that service the copper loops between the access point 345 and the Customer Premises Equipment (CPE) 305, 310, 315. DSLAMs 365, 370, 375 may link locally or via an inter-central office (CO) link to LAC 360.

Traffic enters and exits the DSLAM chassis through ports, each of which is assigned a port address. A virtual circuit or channel (VC) is a logical circuit created to ensure reliable communication between two network devices. A VC is defined by a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI) pair, which is directly tied to a particular DSLAM port used by a particular subscriber.

The LAC 360 is linked to a separate server/memory device 355, herein referred to as an Authentication, Authorization and Accounting (AAA) server 355. The LAC 360 and the AAA server 355 communicate with one-another according to the Remote Access Dial-In User Service (RADIUS) protocol. The specific details of the RADIUS protocol are well known by those of ordinary skill in the art. Moreover, as will be apparent to those of ordinary skill in the art, the RADIUS protocol has limited applicability to the present invention and, therefore a detailed discussion of this protocol is deemed unnecessary. The preferred methods of the present invention described herein are not limited to the use of the RADIUS protocol and other equivalent authentication protocols may be used.

When the LAC 360 receives a PPP authentication request, a virtual circuit profile request generator (not shown in Fig. 4) generates a request packet and a forwarding interface (not shown in Fig. 4) sends a request packet to the AAA server 350. The packet includes the virtual circuit ID 380, 385, 390 associated with the virtual channel used to receive the PPP session. The AAA server 355 receives a request packet from the LAC 360, consults the data bank of virtual circuit profiles contained in its memory and makes

a match based on the virtual circuit ID 380, 385, 390 provided in the request. In order to access the individual profile, a match must be made between the virtual circuit ID 380, 385, 390 in the request packet and the individual profile. If the virtual circuit ID 380, 385, 390 match, and all other requirements are met, the AAA server 350 sends the LAC 360 a virtual circuit profile packet. The virtual circuit profile packet contains all the pertinent information in the port specific virtual circuit profile that enables the LAC 360 to provide the desired service to the user.

10           The virtual circuit profile packet travels from the AAA server 350 to a second receiving interface (not shown in Fig. 4) within the LAC 360 where the LAC 360 serves to create secure channels to private areas of the network for those users who are authorized to use such sites and, an assessor within the LAC 360 makes a determination as to whether or not the virtual circuit profile for DSLAM port has a tunnel selection configuration override attribute associated with it. A calculator determines whether the service associated with the virtual circuit matches the service associated with the domain configuration override attribute. If a tunnel selection configuration override attribute does not exist in the profile, a connection is opened through the home gate 395 of the requested private domain 320. If a tunnel selection configuration override attribute does exist in the virtual circuit profile for the specified DSLAM port, or if the PPP authentication packet does not include a domain name, a tunnel is established with the LNS 400 associated with the DSLAM port.

In accordance with one embodiment of the present invention, the LAC service and the LNS may be implemented using a Cisco 6400 Universal Access Concentrator, available from Cisco Systems, Inc. of San Jose, California.

5

Figures 5 and 6 are flow diagrams that illustrate methods by which a LAC or similar device determines information needed to associate a particular virtual circuit with a tunnel ID.

10           Turning now to Fig. 5, a flow diagram that illustrates a method for static configuration of tunnel-based network connections in accordance with one embodiment of the present invention is presented. According to this embodiment of the present invention, an AAA server maintains a table of domain names indexed by virtual circuit identifiers, and a LAC maintains a table of tunnel IDs indexed by domain names. At 500, a PPP session is received by a LAC or similar device. At 505, an identifier that uniquely describes the virtual circuit used to receive the PPP session (such as a VPI/VCI identifier) is sent to the AAA server. At 510, a domain name that is associated with the unique identifier is received from the AAA server. At 515, a tunnel ID is determined based upon the domain name. The LAC performs a table lookup to obtain the tunnel ID associated with the domain name. At 520, if a tunnel ID has been determined, a tunneling session with the LNS associated with the tunnel ID is established and the PPP session is forwarded to the LNS.

According to another embodiment of the present invention, the information regarding the mapping between virtual circuit ID and tunnel ID is maintained by the LAC or similar device. Figure 6 is a flow diagram that illustrates a method for static configuration of tunnel-based network connections in accordance with one embodiment of the present invention is presented. At 600, a PPP session is received by a LAC or similar device. At 605, a determination is made regarding whether a domain configuration override attribute exists in a virtual circuit profile associated with the DSLAM port used to receive the PPP session. If a domain override attribute exists or if the PPP authentication packet does not include a domain name (610), at 615, the domain is set to the domain indicated in the virtual circuit profile. If a domain override attribute does not exist, the domain is set to the domain used in the PPP authentication packet at 620. The tunnel ID is determined based upon the domain at 625, and the PPP session is forwarded to the LNS at 630.

Figures 7 and 8 are flow diagrams that illustrate methods by which an AAA server or similar device determines information needed to associate a particular virtual circuit with a tunnel ID.

Turning now to Fig. 7, a flow diagram that illustrates a method for determining the domain name associated with a virtual circuit in accordance with one embodiment of the present invention is presented. At 700, a PPP authentication request including a virtual channel ID is received by an AAA server or similar device. At 705, a determination is made regarding whether a domain configuration override attribute exists

in a virtual circuit profile associated with the DSLAM port used to receive the PPP session. If a domain configuration override attribute exists or if the PPP authentication packet does not include a domain name (710), at 715, the domain associated with the virtual channel is returned. If a domain configuration override attribute does not exist, at 5 720, the PPP domain used in the PPP authentication request is returned.

Turning now to Fig. 8, a flow diagram that illustrates a method for determining the tunnel ID associated with a virtual circuit in accordance with one embodiment of the present invention is presented. At 800, a PPP session including a virtual channel ID is 10 received. At 805, a determination is made regarding whether a domain configuration override attribute exists in a virtual circuit profile associated with the DSLAM port used to receive the PPP session. If a domain configuration override attribute exists, at 815, the tunnel ID associated with the virtual channel is returned. If a domain configuration 15 override attribute does not exist, at 820, the PPP domain used in the PPP authentication request is returned.

Figures 9A-9C are tables that illustrate tunnel configuration information that may be stored in a LAC, an AAA server, or other similar devices in accordance with 20 embodiments of the present invention. Figure 9A is a virtual circuit profile table that contains a list of domain names 900 indexed by virtual circuit IDs 905. A domain configuration override attribute 910 determines whether a subscriber is limited to establishing a tunnel with a particular domain.

Figure 9B is a table that includes a list of tunnel IDs 915 indexed by domain names 920. Table 9B may be used in conjunction with table 9A to obtain a tunnel ID 915 associated with a virtual circuit ID 905.

5

Figure 9C is a virtual circuit profile table that contains a list of tunnel IDs 925 indexed by virtual circuit IDs 930. A domain configuration override attribute 935 determines whether a subscriber is limited to establishing a tunnel with a particular domain. In the example, a port having a virtual circuit ID of 94/22 (940) may use tunnel

10 ID 2210 (945) exclusively.

The tunnel selection configuration override attribute is requested by the domain owner to be placed in virtual circuit profiles. It allows the service provider the capability to ensure that a PPP session originating from a DSLAM port allocated to a particular

15 domain can connect with only that particular domain, regardless of what domain name is entered in the PPP authentication packet. This provides added security to the owner of the private domain by lessening the likelihood of an unauthorized access to the home gateway of a corporate intranet. The service provider would have the control over which ports are allocated to which domains. The service provider would also have control over

20 which ports have the tunnel selection configuration attribute in their virtual circuit profile and are, thus, limited to one domain and which virtual circuit profiles do not contain the tunnel selection configuration override attribute and are, thus, free to connect to more than one domain.



Although embodiments of the present invention is have been described with respect to virtual circuits in an ATM networking environment, it should be understood that a virtual circuit assigned to a subscriber in system may be defined in any suitable networking environment using any suitable communication technologies and protocols, without deviating from the scope of the present invention.

In accordance with a specific embodiment of the present invention, the components, process steps, and/or data structures are implemented using software. This implementation is not intended to be limiting in any way. Different implementations may be used and may include other types of operating systems, computing platforms, and/or computer programs. In addition, those of ordinary skill in the art will readily recognize that devices of a less general purpose nature, such as hardwired devices, devices relying on FPGA (field programmable gate array) or ASIC (application specific integrated circuit) technology, or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herewith.

While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.

CLAIMS

What is claimed is:

- 5     1. A method for controlling subscriber access in a network capable of establishing connections with a plurality of services, comprising:
- receiving a communication from a subscriber using a first communication network coupled to a second communication network, said communication optionally including a domain identifier associated with a service on said second
- 10     communication network; and
- authorizing said subscriber to access a service on said second communication network using one of a plurality of virtual circuits, said authorizing based upon a domain configuration override attribute associated with the virtual circuit used to receive said communication from said subscriber.
- 15     2. The method of claim 1 wherein said authorizing further comprises:
- receiving from a memory a virtual circuit profile associated with said virtual circuit; assessing said virtual circuit profile to determine if a domain configuration override attribute exists within said virtual circuit profile; and
- 20     allowing said subscriber to connect exclusively to a service associated with said domain configuration override attribute when said domain configuration override attribute exists within said virtual circuit profile.

3. The method of claim 2, further comprising:  
causing the subscriber to disconnect from all then existing network connections when  
said domain configuration override attribute exists within said virtual circuit  
5        profile and when said domain identifier in said communication does not match  
      said service associated with said domain configuration override attribute.
4. The method of claim 2 wherein said service request comprises a Point-to-Point  
Protocol (PPP) session service request.
- 10    5. The method of claim 4 wherein  
      said PPP session comprises a tunneling session; and  
      said allowing further comprises assigning a tunnel ID.
- 15    6. The method of claim 5 wherein said tunneling session comprises an L2TP session.
7. The method of claim 6 wherein said receiving a virtual circuit profile further  
      comprises performing a table lookup based upon a Virtual Path Identifier (VPI) /  
      Virtual Channel Identifier (VCI) associated with said virtual circuit.
- 20    8. A program storage device readable by a machine, embodying a program of  
      instructions executable by the machine to perform a method to control subscriber  
      access in a network capable of establishing connections with a plurality of services,  
      the method comprising:  
25        receiving a communication from a subscriber using a first communication network  
          coupled to a second communication network, said communication optionally

including a domain identifier associated with a service on said second  
communication network; and

authorizing said subscriber to access a service on said second communication

5 network using one of a plurality of virtual circuits, said authorizing based upon a  
domain configuration override attribute associated with the virtual circuit used to  
receive said communication from said subscriber.

9. The program storage device of claim 8 wherein said authorizing further comprises:

10 receiving from a memory a virtual circuit profile associated with said virtual circuit;  
assessing said virtual circuit profile to determine if a domain configuration override  
attribute exists within said virtual circuit profile; and  
allowing said subscriber to connect exclusively to a service associated with said  
domain configuration override attribute when said domain configuration override  
15 attribute exists within said virtual circuit profile.

10. The program storage device of claim 9, further comprising:

causing the subscriber to disconnect from all then existing network connections when  
said domain configuration override attribute exists within said virtual circuit  
20 profile and when said domain identifier in said communication does not match  
said service associated with said domain configuration override attribute.

11. The program storage device of claim 9 wherein said service request comprises a  
Point-to-Point Protocol (PPP) session service request.

25

12. The program storage device of claim 11 wherein  
 said PPP session comprises a tunneling session; and  
 said allowing further comprises assigning a tunnel ID.

5

13. The program storage device of claim 12 wherein said tunneling session comprises an  
 L2TP session.

14. The program storage device of claim 13 wherein said receiving a virtual circuit  
 10 profile further comprises performing a table lookup based upon a Virtual Path  
 Identifier (VPI) / Virtual Channel Identifier (VCI) associated with said virtual circuit.

15. An apparatus for controlling subscriber access in a network capable of establishing  
 connections with a plurality of services, the apparatus comprising:  
 15 means for receiving a communication from a subscriber using a first communication  
 network coupled to a second communication network, said communication  
 optionally including a domain identifier associated with a service on said second  
 communication network; and  
 means for authorizing said subscriber to access a service on said second  
 20 communication network using one of a plurality of virtual circuits, said  
 authorizing based upon a domain configuration override attribute associated with  
 the virtual circuit used to receive said communication from said subscriber.

16. The apparatus of claim 15 wherein said means for authorizing further comprises:

means for receiving from a memory a virtual circuit profile associated with said  
virtual circuit;

5 means for assessing said virtual circuit profile to determine if a domain configuration  
override attribute exists within said virtual circuit profile; and

means for allowing said subscriber to connect exclusively to a service associated with  
said domain configuration override attribute when said domain configuration  
override attribute exists within said virtual circuit profile.

10

17. The apparatus of claim 16, further comprising:

means for causing the subscriber to disconnect from all then existing network  
connections when said domain configuration override attribute exists within said  
virtual circuit profile and when said domain identifier in said communication  
15 does not match said service associated with said domain configuration override  
attribute.

18. The apparatus of claim 16 wherein said service request comprises a Point-to-Point  
Protocol (PPP) session service request.

20

19. The apparatus of claim 18 wherein

said PPP session comprises a tunneling session; and

said means for allowing further comprises assigning a tunnel ID.

20. The apparatus of claim 19 wherein said tunneling session comprises an L2TP session.

21. The apparatus of claim 20 wherein said means for receiving a virtual circuit profile

5 further comprises a means for performing a table lookup based upon a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI) associated with said virtual circuit.

22. An access server capable of forcing subscribers of a communications system to gain access exclusively to a domain network associated with a virtual circuit, said access  
10 server comprising:

an authorizer capable of granting service authorization to said subscribers based upon a virtual circuit used to make a service request;

a virtual circuit profile request generator capable of generating virtual circuit profile requests;

15 an assessor capable of assessing said requested virtual circuit profile for a domain configuration override attribute; and

a calculator capable of determining whether the service associated with said virtual circuit matches the service associated with said domain configuration override attribute.

20

23. The access server of claim 22, further comprising:

a receiving interface capable of accepting said service requests;

a forwarding interface capable of sending said virtual circuit profile requests to a memory bank; and

25 a second receiving interface capable of accepting requested virtual circuit profiles.

24. The access server of claim 22 wherein said service request comprises a Point-to-Point Protocol (PPP) session service request.

5 25. The access server of claim 23 wherein  
said PPP session comprises a tunneling session; and  
said calculator is capable of assigning a tunnel ID.

10 26. The access server of claim 24 wherein said tunneling session comprises an L2TP  
session.

27. The access server of claim 25 wherein said assessor is capable of performing a table  
lookup based upon a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI)  
associated with said virtual circuit.

15 28. The access server of claim 26 wherein said receiving interface comprises at least one  
access multiplexer, each access multiplexer having a plurality of inputs for receiving  
a service request, each of said inputs being associated with a particular subscriber  
virtual circuit.

20 29. The access server of claim 23 wherein said memory bank and said access server  
communicate using the Remote Authorization Dial-In User Service (RADIUS)  
protocol.



30. An access server capable of forcing subscribers of a communications system to gain access exclusively to a domain network associated with a virtual circuit, said access server comprising:

- 5 a memory device capable of storing a plurality of virtual circuit profiles, said virtual circuit profiles capable of having a domain configuration override attribute associated with subscriber authorized services;
- an authorizer capable of granting service authorization to said subscribers based upon a virtual circuit used to make a service request;
- 10 a virtual circuit profile request generator capable of generating virtual circuit profile requests;
- an assessor capable of assessing said requested virtual circuit profile for a domain configuration override attribute; and
- a calculator capable of determining whether the service associated with said virtual circuit matches the service associated with said domain configuration override attribute.
- 15

31. The access server of claim 29, further comprising:

- 20 a receiving interface capable of accepting said service requests;
- a forwarding interface capable of sending said virtual circuit profile requests to a memory bank; and
- a second receiving interface capable of accepting requested virtual circuit profiles.

32. The access server of claim 29 wherein said service request comprises a Point-to-Point Protocol (PPP) session service request.

5 33. The access server of claim 29 wherein  
said PPP session comprises a tunneling session; and  
said calculator is capable of assigning a tunnel ID.

10 34. The access server of claim 32 wherein said tunneling session comprises an L2TP  
session.

35. The access server of claim 33 wherein said assessor is capable of performing a table  
lookup based upon a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI)  
associated with said virtual circuit.

15 36. The access server of claim 34 wherein said receiving interface comprises at least one  
access multiplexer, each access multiplexer having a plurality of inputs for receiving  
a service request, each of said inputs being associated with a particular subscriber  
virtual circuit.

20

ABSTRACT OF THE DISCLOSURE

A method for controlling subscriber access in a network capable of establishing  
5 connections with multiple services includes receiving a communication from a subscriber  
using a first communication network coupled to a second communication network, the  
communication optionally including a domain identifier associated with a service on the  
second communication network, and authorizing the subscriber to access a service on the  
second communication network using a virtual circuit. The authorization is based upon a  
10 domain configuration override attribute associated with the virtual circuit used to receive  
the communication from the subscriber. An access server capable of forcing subscribers  
of a communications system to gain access exclusively to a domain network associated  
with a virtual circuit includes an authorizer to grant service authorization to the  
subscribers based upon a virtual circuit used to make a service request, a virtual circuit  
15 profile request generator to generate virtual circuit profile requests and a calculator to  
determine whether the service associated with the virtual circuit matches the service  
associated with a domain configuration override attribute.

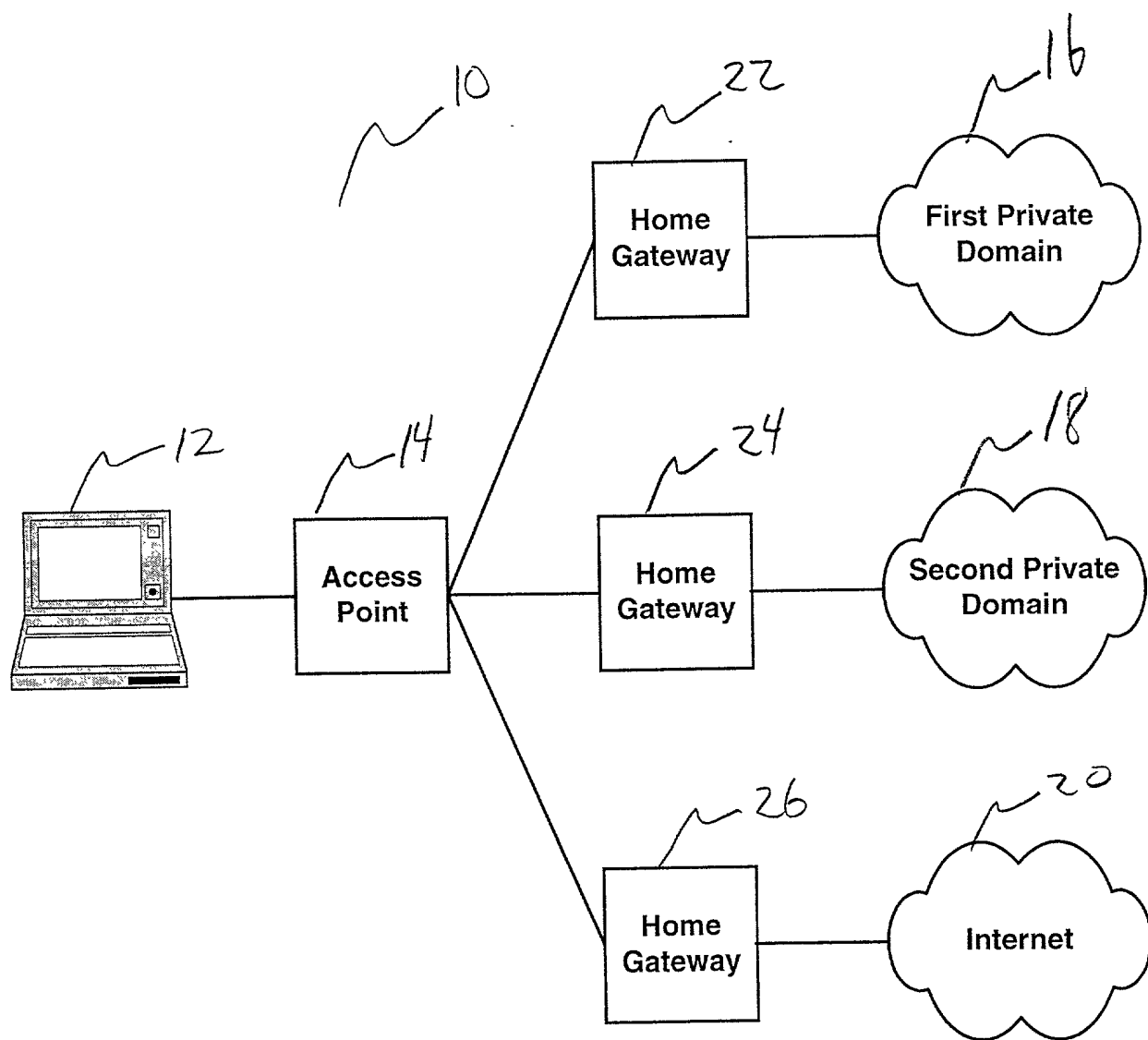


Fig. 1

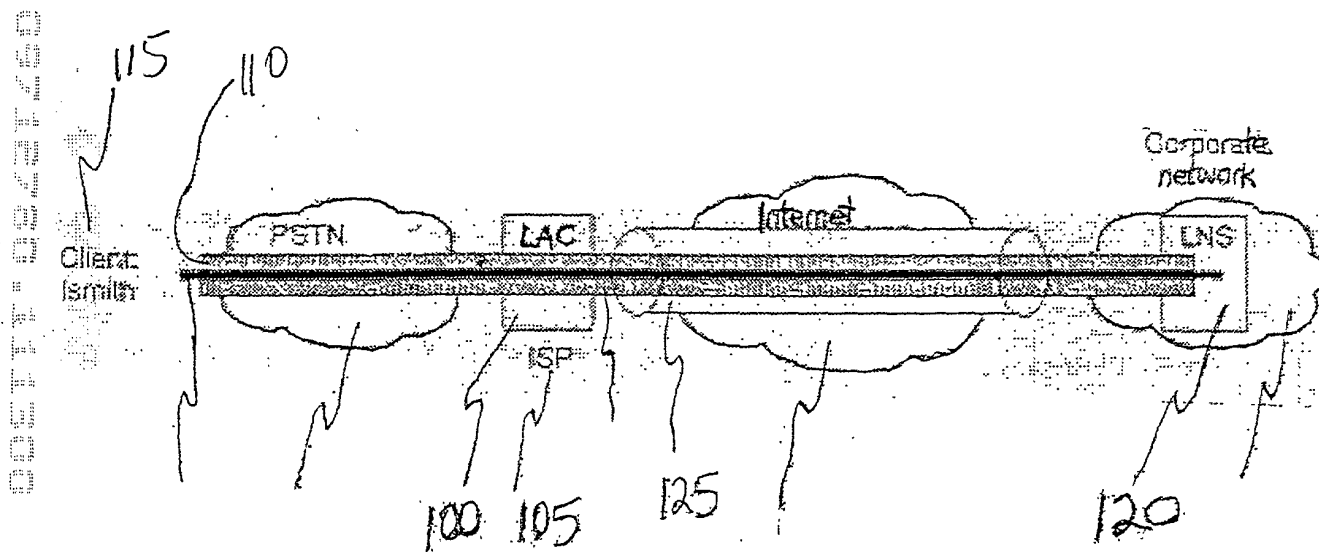


Fig. 2

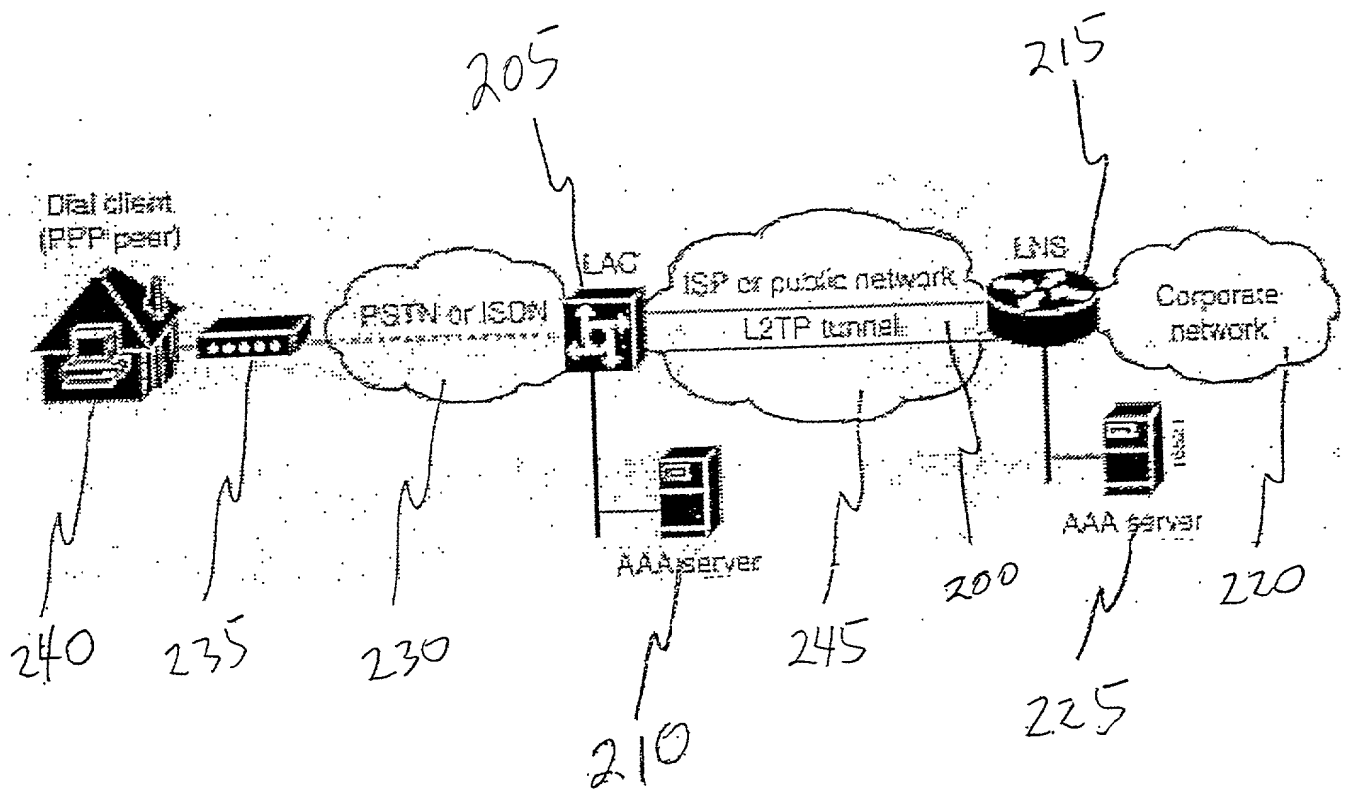


Fig. 3

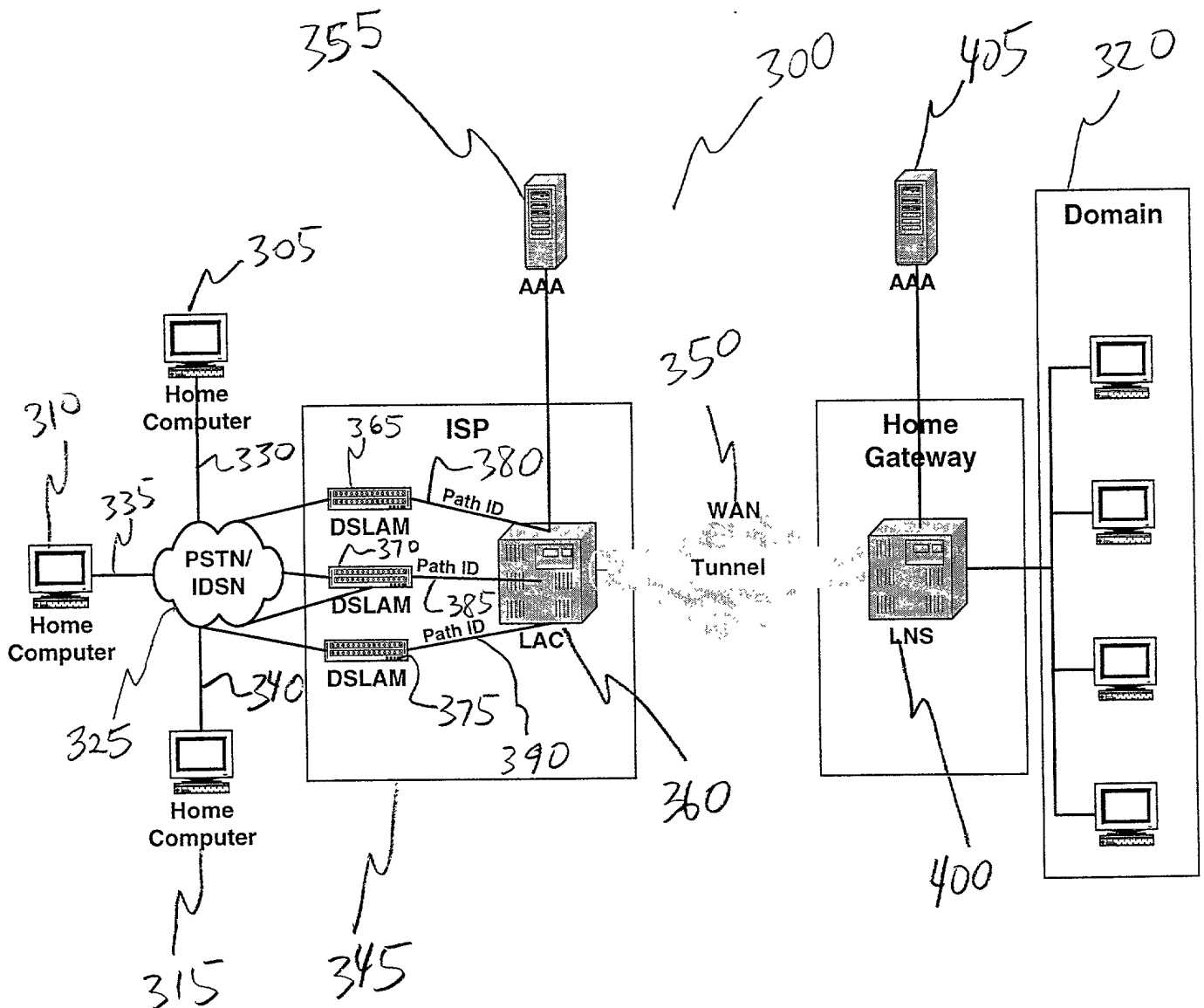


Fig. 4

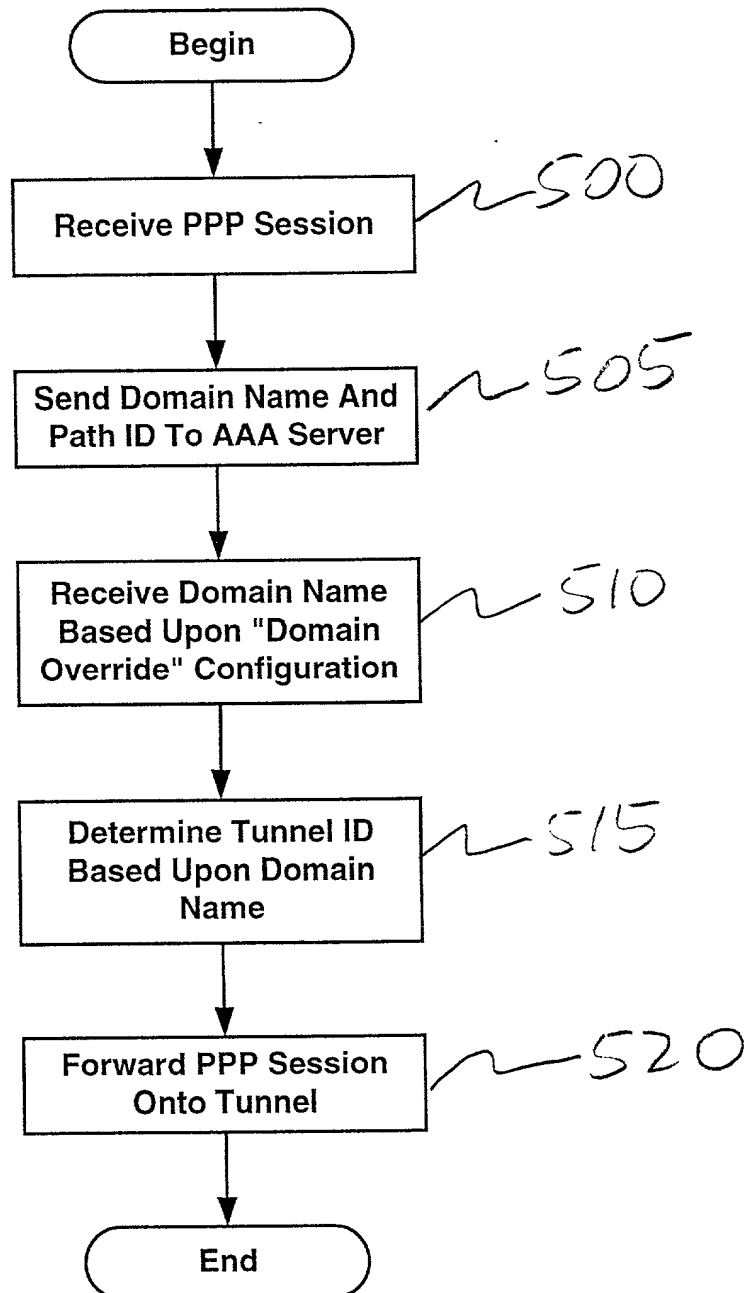


Fig. 5



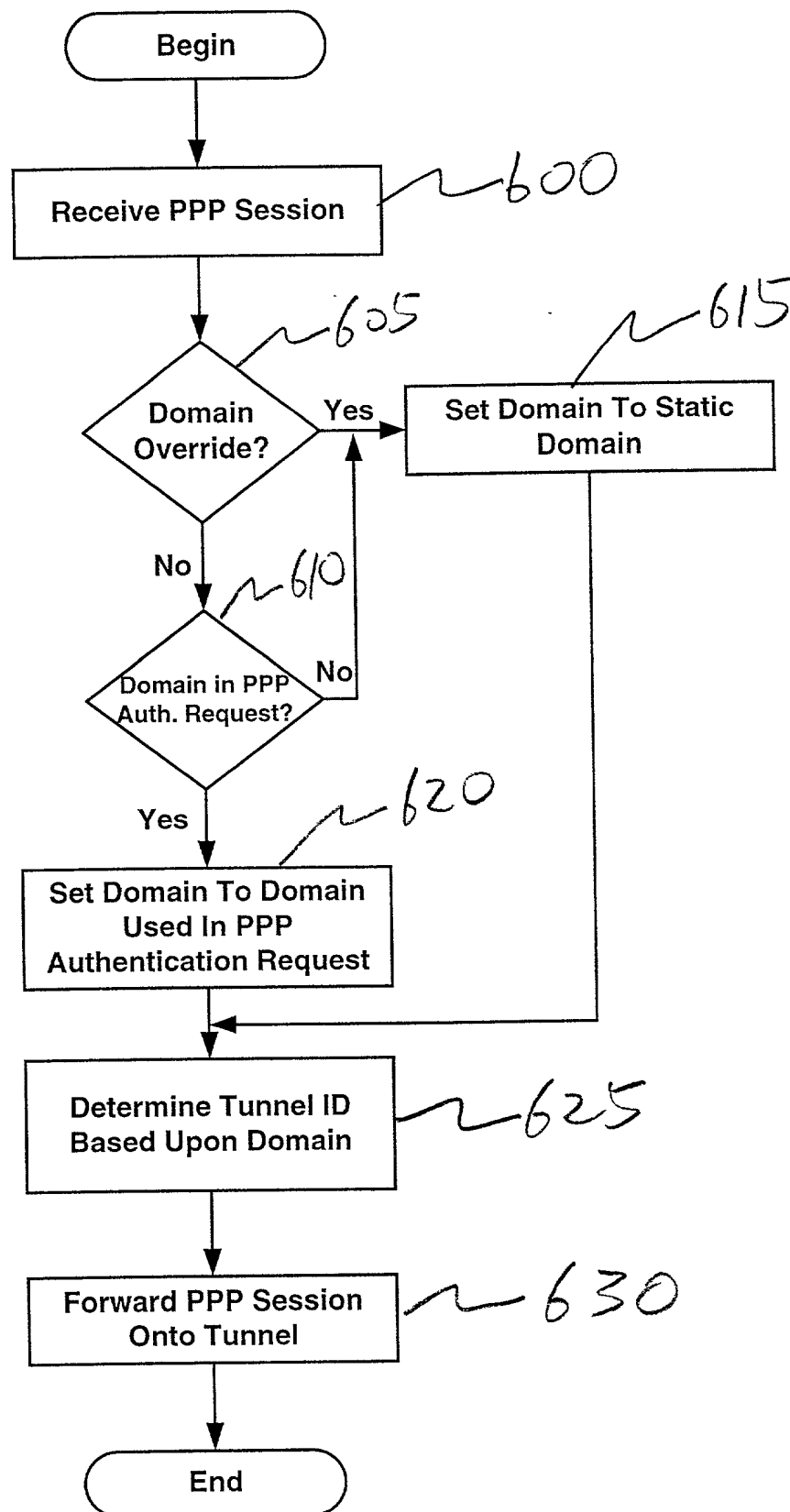


Fig. 6

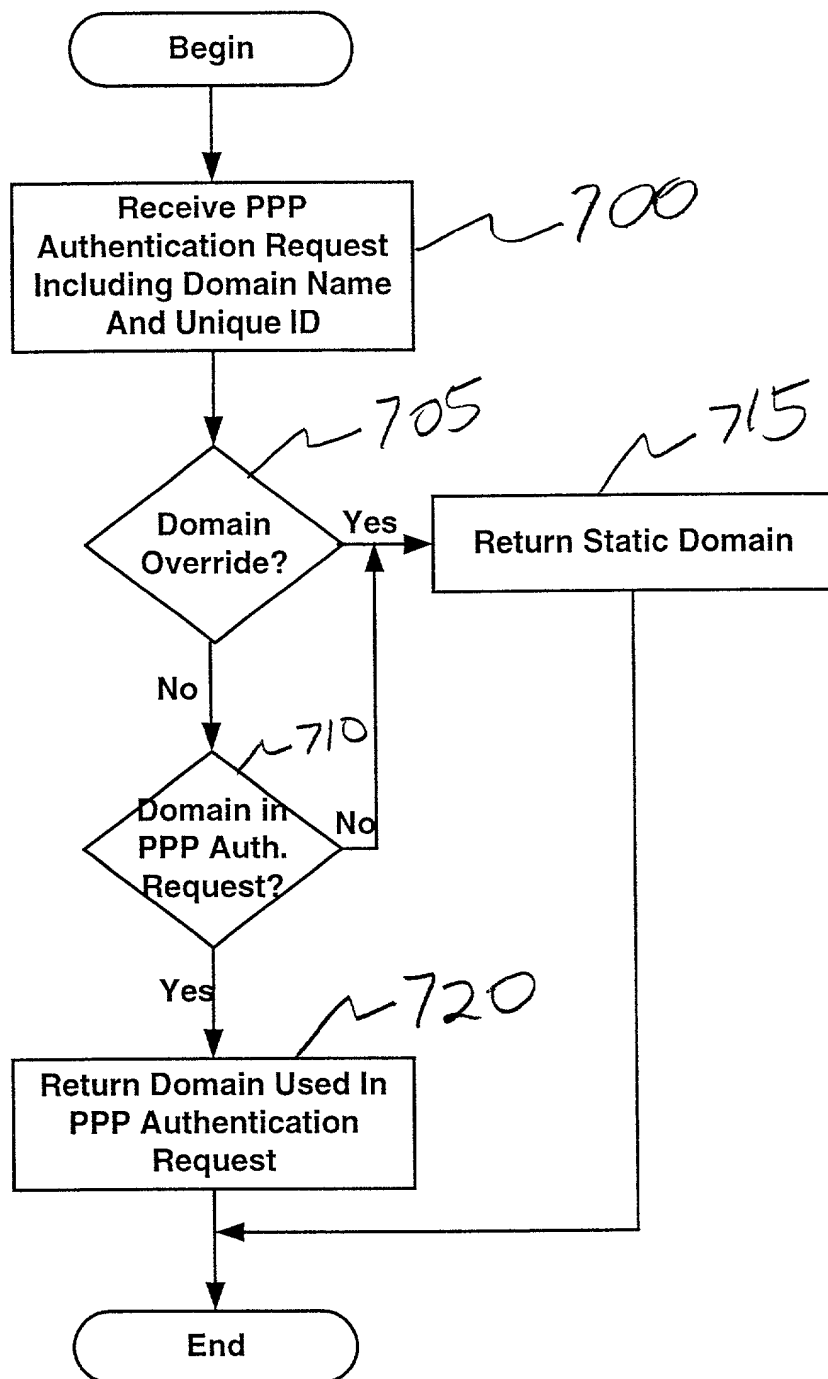


Fig. 7

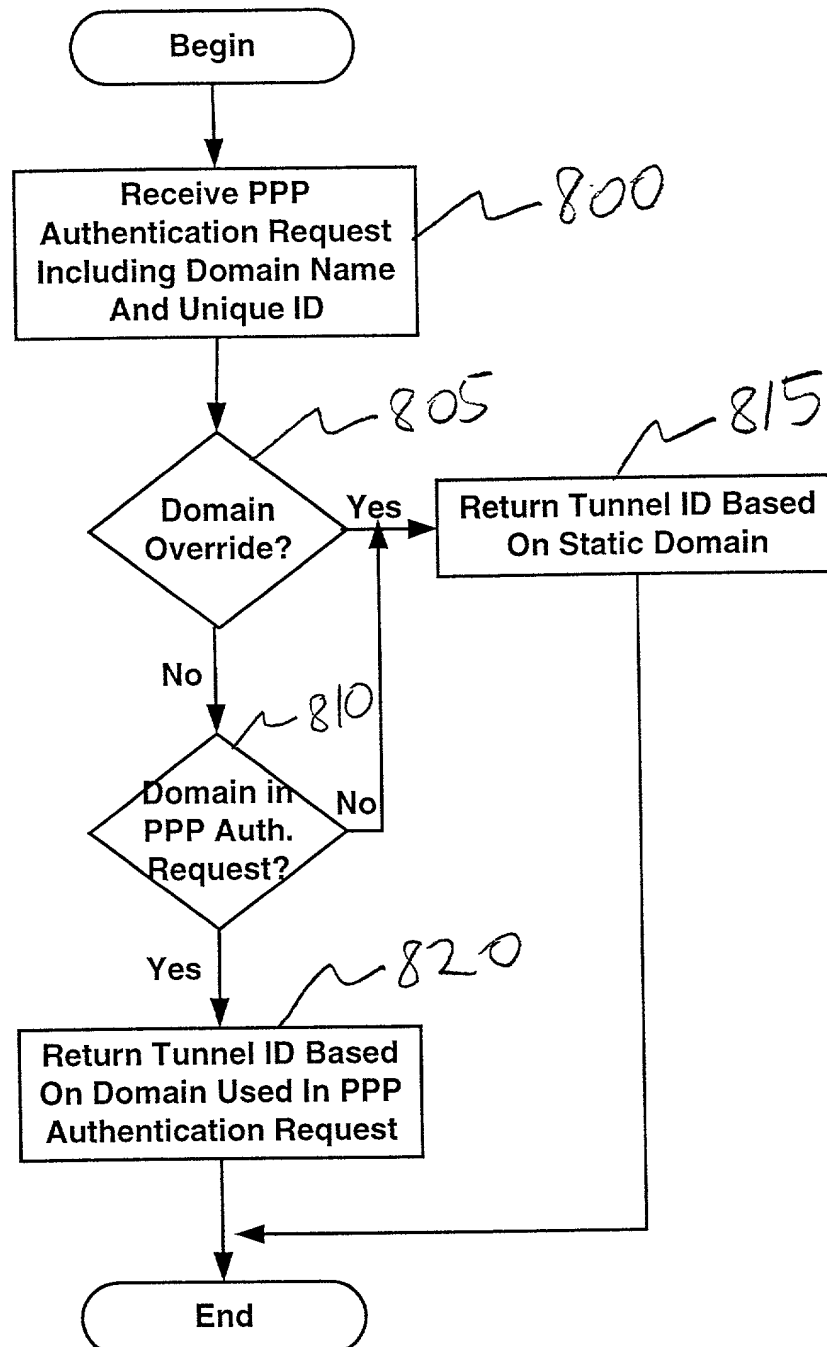


Fig. 8

905 910 900

| VPI/VCi | Domain Configuration Override | Domain Name |
|---------|-------------------------------|-------------|
| 10/2    | Yes                           | corpA.com   |
| 33/1    | Yes                           | corpA.com   |
| 94/22   | Yes                           | corpC.com   |

Fig. 9A

920 915

| Domain Name | Tunnel ID |
|-------------|-----------|
| corpA.com   | 4578      |
| corpB.com   | 3948      |
| corpC.com   | 2210      |

Fig. 9B

930 935 925

| VPI/VCi | Domain Configuration Override | Tunnel ID |
|---------|-------------------------------|-----------|
| 10/2    | Yes                           | 4578      |
| 33/1    | Yes                           | 4578      |
| 94/22   | Yes                           | 2210      |

940 945

Fig. 9C